EduGroupe
Accompagner pour réussir

Analyse des risques

Durée : 4 jours (28 heures)

CONNAISSANCES PREALABLES

- Connaissances générales des systèmes d'information.
- Connaissances de base en cybersécurité et gouvernance des SI.
- Une première expérience dans la gestion de projets, l'exploitation informatique ou la sécurité des systèmes d'information est recommandée.

PROFIL DES STAGIAIRES

- RSSI et responsables cybersécurité
- DSI et responsables informatiques
- Responsables risques et conformité
- Auditeurs internes et consultants sécurité
- Chefs de projets SI
- Correspondants sécurité
- Toute personne impliquée dans la gestion des risques liés aux systèmes d'information.

OBJECTIFS

À l'issue de la formation, les participants seront capables de :

- Comprendre les principes de gestion des risques selon ISO/IEC 27005.
- Maîtriser le cycle complet d'analyse et de traitement des risques.
- Identifier les actifs, menaces, vulnérabilités et impacts métiers.
- Réaliser une analyse de risques conforme aux référentiels internationaux.
- Mettre en œuvre la méthode EBIOS Risk Manager.
- Construire des scénarios stratégiques et opérationnels.
- Définir et prioriser les mesures de traitement des risques.
- Présenter les résultats d'une analyse de risques à la direction.
- Préparer une organisation à une démarche de conformité ISO 27001, NIS2 ou DORA.

CERTIFICATION PREPAREE

ISO27005 Risk Manager, certification officielle PECB (1 passage par candidat, 2e passage gratuit en cas d'échec au 1er, dans un délai d'un an).

METHODES PEDAGOGIQUES

- Alternance d'apports théoriques et d'études de cas.
- Ateliers collaboratifs de construction d'analyses de risques.
- Exercices pratiques basés sur des scénarios réalistes.
- Travaux de groupe autour de cas d'entreprise.
- Utilisation de matrices et outils d'analyse des risques.

- Étude fil rouge permettant de mettre en œuvre l'ensemble de la démarche.

FORMATEUR

- Consultant expert en gouvernance de la sécurité des systèmes d'information, gestion des risques et conformité réglementaire disposant d'une expérience significative dans la réalisation d'analyses de risques selon les méthodologies ISO 27005, EBIOS Risk Manager et ISO 31000. Il est certifié sur ISO 27005 Risk Manager et EBIOS Risk Manager. Formateur habilité par PECB.

METHODE D'EVALUATION DES ACQUIS

- Questionnaire de positionnement en début de formation.
- Validation continue des acquis à travers les ateliers et exercices.
- Études de cas et travaux pratiques réalisés en groupe.
- Quiz intermédiaires de validation des connaissances.
- Cas pratique fil rouge réalisé durant la formation.
- Questionnaire final d'évaluation des acquis.

CONTENU DU COURS

Jour 1 : Fondamentaux de la gestion des risques selon ISO 27005 (7h)

Module 1 : Gouvernance et gestion des risques de sécurité (2h)

Objectifs

- Comprendre les enjeux de la gestion des risques.
- Positionner l'analyse de risques dans une démarche de gouvernance SSI.

Contenu

- Gouvernance de la sécurité.
- Concepts fondamentaux du risque.
- ISO 31000 et ISO 27005.
- Gestion des risques et création de valeur.
- Place de l'analyse de risques dans l'ISO 27001.

Mise en pratique

Brainstorming collectif :

- Identification des risques stratégiques et opérationnels d'une organisation.

Module 2 : Identifier les actifs, les menaces et les vulnérabilités (3h)

Objectifs

- Cartographier les éléments critiques d'un système d'information.

Contenu

- Actifs métiers et supports.
- Processus critiques.
- Sources de menaces.
- Vulnérabilités techniques, humaines et organisationnelles.
- Impacts métiers.

Mise en pratique

Atelier :

- Cartographie des actifs et identification des risques associés.

Module 3 : Évaluation et appréciation des risques (2h)

Objectifs

- Évaluer la vraisemblance et l'impact des risques.

Contenu

- Critères d'évaluation.
- Matrices de risques.
- Criticité.
- Acceptabilité des risques.
- Priorisation.

Mise en pratique

Travaux pratiques :

- Construction d'une matrice d'évaluation des risques.

Jour 2 : Mettre en œuvre une démarche ISO 27005 (7h)

Module 4 : Réaliser une analyse de risques ISO 27005 (3h)

Objectifs

- Appliquer les étapes de la méthode ISO 27005.

Contenu

- Contexte et périmètre.
- Identification des risques.
- Estimation et évaluation.
- Documentation des résultats.
- Communication des risques.

Mise en pratique

Atelier :

- Réalisation guidée d'une analyse de risques.

Module 5 : Traitement et gestion des risques (2h)

Objectifs

- Définir les mesures de sécurité adaptées.

Contenu

- Réduction du risque.
- Acceptation.
- Transfert.
- Évitement.
- Déclaration d'applicabilité (SoA).

Mise en pratique

Travail en groupe :

- Élaboration d'un plan de traitement des risques.

Module 6 : Reporting et pilotage des risques (2h)

Objectifs

- Présenter les résultats à la direction.

Contenu

- Tableaux de bord.
- Communication des risques.
- Indicateurs.
- Pilotage et amélioration continue.

Mise en pratique

Atelier :

- Construction d'un reporting de risques pour un comité de direction.

Jour 3 : Maîtriser EBIOS Risk Manager (7h)

Module 7 : Présentation de la méthode EBIOS Risk Manager (1h)

Objectifs

- Comprendre les principes et la logique d'EBIOS RM.

Contenu

- Historique de la méthode.
- Positionnement vis-à-vis d'ISO 27005.
- Concepts clés.
- Vue d'ensemble des cinq ateliers.

Mise en pratique

Échanges et retours d'expérience.

Module 8 : Atelier 1 – Cadrage et socle de sécurité (2h)

Objectifs

- Définir le périmètre et les enjeux.

Contenu

- Valeurs métier.
- Événements redoutés.
- Référentiel de sécurité existant.

Mise en pratique

Travaux pratiques :

- Réalisation de l'atelier 1 sur un cas d'étude.

Module 9 : Atelier 2 – Sources de risque (2h)

Objectifs

- Identifier les acteurs menaçants.

Contenu

- Écosystème.
- Parties prenantes.
- Sources de risques.
- Capacités et motivations.

Mise en pratique

Atelier :

- Cartographie des sources de risque.

Module 10 : Atelier 3 – Scénarios stratégiques (2h)

Objectifs

- Construire des scénarios de menace crédibles.

Contenu

- Objectifs des attaquants.
- Chemins d'attaque.
- Scénarios stratégiques.

Mise en pratique

Travaux pratiques :

- Construction de scénarios stratégiques.

Jour 4 : Mise en œuvre avancée d'EBIOS RM et synthèse (7h)

Module 11 : Atelier 4 – Scénarios opérationnels (2h)

Objectifs

- Détailler les scénarios d'attaque.

Contenu

- Vulnérabilités exploitables.
- Chemins d'attaque.
- Conditions de réussite.

Mise en pratique

Atelier :

- Construction de scénarios opérationnels.

Module 12 : Atelier 5 – Traitement du risque (2h)

Objectifs

- Définir les mesures de sécurité.

Contenu

- Mesures de réduction.
- Mesures organisationnelles.
- Mesures techniques.
- Priorisation des actions.

Mise en pratique

Travaux pratiques :

- Élaboration d'un plan de traitement.

Module 13 : Cas pratique complet ISO 27005 & EBIOS RM (2h)

Objectifs

- Mettre en œuvre l'ensemble de la démarche.

Mise en pratique

Cas fil rouge :

- Analyse des risques.
- Ateliers EBIOS.
- Évaluation.
- Traitement.
- Reporting.

Module 14 : Restitution et préparation à la certification (1h)

Objectifs

- Consolider les acquis.
- Préparer l'examen de certification.

Mise en pratique

Quiz blanc et débriefing collectif.

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à mailto:referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.